Amendments

In the Claims:

What is claimed is:

[c1] (Currently Amended) A method of preventing unauthorized access to a computer system, comprising:

receiving a data packet at a firewall, where the data packet comprises a frame field, a header, a body, and a trailer;

passively copying the data packet at the firewall, where the passive copying leaves the frame field, the header, the body, and the trailer of the data packet unchanged so that there is no indication of the firewall in the data packet;

analyzing the passively copied data packet with the firewall to determine if the data packet is authorized to access the computer system;

sending an authorized data packet to the computer system; and

denying access of an unauthorized data packet to the computer system.

[c2] (Original) The method of claim 1, further comprising:

dropping the unauthorized data packet.

[c3] (Original) The method of claim 1, further comprising:

logging the attempted access to the computer system of the unauthorized data packet.

[c4] (Original) The method of claim 1, wherein the computer system is a network.

[c5] (Original) The method of claim 1, wherein the data packet is analyzed by a pattern matching system.

[c6] (Currently Amended) A method of preventing unauthorized access to a computer system, comprising:

step ~~of~~ for receiving data;

step ~~of~~ for passively copying the data, where the passive copying leaves the data unchanged so that there is no indication of the firewall in the data packet ;

step ~~of~~ for analyzing the passively copied data for authorization to access the computer system; ~~and~~

step ~~of~~ for allowing access to the computer system for authorized data; and

step ~~of~~ for denying access to the computer system for unauthorized data.

[c7] (Currently Amended) The method of claim 6, further comprising:

step ~~of~~ for dropping unauthorized data.

[c8] (Currently Amended) The method of claim 6, further comprising:

step ~~of~~ for logging an attempt to access the computer system by unauthorized data.

[c9] (Original) A method of remotely managing a firewall, comprising:

receiving a control data packet at the firewall from a remote location;

passively copying the control data packet at the firewall, where the passive copying leaves all content of the control data packet unchanged so that there is no indication of the firewall in the control data packet;

analyzing the passively copied control data packet to determine if the control data packet is authorized to access the firewall; and

allowing an authorized control data packet to control the firewall.

[c10] (Original) The method of claim 9, further comprising:

dropping the authorized control data packet.

[c11] (Original) The method of claim 9, wherein the control data packet is analyzed for a password.

[c12] (Original) The method of claim 9, wherein the control data packet contains a false origination address.

[c13] (Original) The method of claim 9, wherein the control data packet contains a destination address that is protected by the firewall.

[c14] (Currently Amended) A method of remotely managing a firewall, comprising:

step ~~of~~ for receiving control data at the firewall from a remote location;

step ~~of~~ for passively copying the control data, where the passive copying leaves all content of the control data unchanged so that there is no indication of the firewall in the control data;

step ~~of~~ for analyzing the passively copied control data to determine if the control data is authorized to access the firewall; and

step ~~of~~ for allowing authorized control data to access the firewall.

[c15] (Currently Amended) The method of claim 14, further comprising:

step ~~of~~ for dropping the authorized control data.